UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of A black iPhone 13 Pro Max with telephone number 562-939-3630 and IMEI number 357447881170809, in the custody of the DEA in Los Angeles, California, as described in Attachment A.	)	Case No. 2:23-mj-01969

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841	Possession with Intent to Distribute Controlled Substances
21 U.S.C. § 846	Conspiracy and Attempt to Distribute Controlled Substances

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Christopher Prossnitz

Applicant's signature

Christopher Prossnitz, FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Hon. Alexander F. MacKinnon, U.S. Magistrate Judge

Printed name and title

AUSA: David C. Lachman (x5564)

ATTACHMENT A

DEVICE TO BE SEARCHED

1. A black iPhone 13 Pro Max with telephone number 562-939-3630 and IMEI number 357447881170809 (the "SUBJECT DEVICE"), seized from Steve JAIMES on March 31, 2023, and currently maintained in the custody of the Drug Enforcement Administration in Los Angeles, California.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (Possession with Intent to Distribute Controlled Substances) and 21 U.S.C. § 846 (Conspiracy and Attempt to Distribute Controlled Substances (the "Subject Offenses"), namely:

a. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

d. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

f. Contents of any calendar or date book;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

h. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

i. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR THE SUBJECT DEVICES

3. In searching the SUBJECT DEVICE (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The "search team" will, in its discretion, either search the SUBJECT DEVICE on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope

of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Criffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

g. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that a SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may

retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not

apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Christopher Prossnitz, being duly sworn, declare and state as follows:

I. BACKGROUND OF AFFIANT

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since 2020. I received extensive instruction at the FBI Academy in Quantico, Virginia, regarding the investigation of violations of the Controlled Substances Act and criminal conspiracies involving the smuggling and distribution of narcotics and dangerous drugs.

2. I am currently assigned to the Los Angeles High Intensity Drug Trafficking Area, Southern California Drug Task Force (the "HIDTA Task Force"). The HIDTA Task Force is comprised of agents and officers from federal, state, and local law enforcement agencies focused on investigating large-scale narcotics trafficking.

3. During the course of my employment with FBI, I have conducted or assisted in investigations into the unlawful importation, manufacture, possession with intent to distribute, and distribution of narcotics and other controlled substances, and conspiracies associated with narcotics and controlled substance offenses. I have used a variety of investigative techniques and resources, including, but not limited to, search warrants, physical surveillance, undercover operations, toll analysis, and electronic and video surveillance.

II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of a warrant to search a black iPhone 13 Pro Max with telephone number 562-939-3630 and IMEI number 357447881170809 (the "SUBJECT DEVICE") in the custody of the Drug Enforcement Administration ("DEA") in Los Angeles, California, as more fully described in Attachment A.

5. The requested search warrant seeks authorization to seize evidence, fruits or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) (Possession with Intent to Distribute Controlled Substances) and 846 (Conspiracy and Attempt to Distribute Controlled Substances) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates and times are approximate.

III. SUMMARY OF PROBABLE CAUSE

7. In or about August 2022, members of HIDTA Task Force began investigating Luis Hugo Parra Montes ("PARRA MONTES"), a

poly-drug trafficker based out of Culiacan in Sinaloa, Mexico. According to a confidential source working with the FBI ("CS-1"),[1] PARRA MONTES facilitates drug transactions by connecting drug customers with U.S.-based couriers who have drugs available for sale. In March 2023, PARRA MONTES agreed to arrange the sale of 10,000 fentanyl pills to CS-1 on March 16, 2023. On the morning of March 16, 2023, PARRA MONTES told CS-1 that he had provided CS-1's telephone number to a U.S.-based drug courier who would be calling CS-1. Shortly thereafter, CS-1 received a telephone call from the user of SUBJECT DEVICE, subsequently identified as Steve JAIMES ("JAIMES"). Over a series of telephone calls and text messages, JAIMES, using the SUBJECT DEVICE, agreed to meet CS-1's associate, another confidential source working with the FBI ("CS-2"),[2] in Downey, California, later that day to deliver the 10,000 fentanyl pills. JAIMES then met CS-2 outside a Walmart store in Downey and gave CS-2 a large plastic bag filled with approximately 10,000 blue pills, which are suspected to contain fentanyl.

[1] CS-1 is a defendant in a pending federal narcotics case in the District of Oregon. CS-1 has pleaded guilty in that case and is cooperating with law enforcement in an attempt to obtain a reduced sentence. CS-1 was also arrested on state drug charges in 2014, which were dismissed. The information provided by CS-1 relating to this investigation has previously shown to be reliable and accurate.

[2] CS-2 is a defendant in a pending federal narcotics case in the District of Nevada. CS-2 has pleaded guilty in that case, and is cooperating with law enforcement in an attempt to obtain a reduced sentence. Agents have taken steps to corroborate information provided by CS-2, and the information provided by CS-2 relating to this investigation has shown to be reliable and accurate.

8. On March 31, 2023, Buena Park Police Department ("BPPD") officers arrested JAIMES in a buy-bust operation coordinated with Homeland Security Investigations ("HSI"). JAIMES used the SUBJECT DEVICE to coordinate the narcotics transaction on March 31, 2023, and officers found the SUBJECT DEVICE in JAIMES's vehicle when they arrested him. During a Mirandized interview, JAIMES signed a federal consent form allowing agents to search the SUBJECT DEVICE.

IV. STATEMENT OF PROBABLE CAUSE

9. Based on my review of law enforcement reports, conversations with other law enforcement agents and confidential sources, and my own knowledge of the investigation, I am aware that in February 2022, CS-1 informed law enforcement that he/she had been contacted by PARRA MONTES to arrange narcotics transactions. CS-1 and PARRA MONTES know each other from narcotics transactions before the CS's arrest in 2014. PARRA MONTES is unaware that CS-1 is cooperating with law enforcement and believes that CS-1 is a drug purchaser. According to CS-1, PARRA MONTES is a poly-drug trafficker based out of Culiacan in Sinaloa, Mexico, who facilitates narcotics transactions by connecting clients with U.S.-based couriers who have narcotics available for sale.

10. Based on my meetings with CS-1 and my consensual monitoring of CS-1's communications, I know the following:

a. PARRA MONTES contacts CS-1 on a Facebook messenger account with vanity name "Luis Hugo Parra Montes."

PARRA MONTES also utilizes the Mexican cellular telephone number 52-667-539-2218 (the "2218 number").

b. During the weeks of March 6 and March 13, 2023, PARRA MONTES communicated with CS-1 via Facebook Messenger to coordinate the sale of 10,000 fentanyl pills from one of PARRA MONTES's associates to CS-1 for $4,800. Over the course of those communications, PARRA MONTES and CS-1 agreed that the deal would take place on Thursday, March 16, 2023.

c. At approximately 7:25 p.m. on March 15, 2023, CS-1 called PARRA MONTES using the 2218 number to confirm that the sale of 10,000 fentanyl pills would take place the following day, March 16, 2023. PARRA MONTES instructed CS-1 to pay the courier who delivers the fentanyl pills $3,300, and to either give the remaining $1,500 to "Martha," who would then send PARRA MONTES the money, or to send the $1,500 directly to PARRA MONTES in Culiacan. PARRA MONTES informed CS-1 that PARRA MONTES would pass on the courier's telephone number to CS-1 early the following morning.

d. On March 16, 2023, between approximately 8:31 a.m. and 11:42 a.m., CS-1 had approximately six telephone conversations with PARRA MONTES using the 2218 number. Over the course of these conversations, PARRA MONTES confirmed that he had provided CS-1's telephone number to the courier and that the courier would be calling CS-1 shortly.

e. At approximately 11:48 a.m. on March 15, 2023, CS-1 received a phone call from the SUBJECT DEVICE's number. Based on my review of subsequent T-Mobile records obtained via

administrative subpoena, this cellular telephone number is subscribed to Steve JAIMES at 6900 Templeton St, Huntington Park, California 90255.

f. Based on my review of DMV database records, I know that Steve JAIMES, date of birth November 20, 1983, is a Hispanic male, is approximately 5'11" tall, weighs approximately 240 pounds, and has black hair and brown eyes.

g. On March 16, 2023, between approximately 11:48 a.m. and 12:09 p.m., the user of the SUBJECT DEVICE communicated with CS-1 approximately eight times via telephone calls and text messages. Over the course of these communications, the user of the SUBJECT DEVICE agreed to meet with CS-1 in Downey, California, at approximately 1 p.m. CS-1 advised that he/she would be sending his/her associate, CS-2, to complete the narcotics transaction. CS-1 provided the address of 9050 Apollo Way, Downey, California 90242, and the user of the SUBJECT DEVICE confirmed that he would be at that location at 1 p.m.

h. Between approximately 12:48 p.m. and 1:11 p.m., the user of the SUBJECT DEVICE communicated with CS-1 approximately five times via telephone calls and text messages. Over the course of these communications, CS-1 explained that CS-2 was waiting in front of the Wal-Mart across the street from the 9050 Apollo Way address. CS-1 described CS—2's appearance and the vehicle CS-2 was driving. The user of the SUBJECT DEVICE advised that he had arrived at the Wal-Mart and was driving a green Nissan Rogue. CS-1 also stated that CS-2 was by the "outdoors" section of the Wal-Mart entrance.

11. Based on my participation in the controlled narcotics purchase on Thursday, March 16, 2023, I know that at approximately 1:12 p.m., an unidentified male driving a green Nissan Rogue parked next to CS-2's vehicle. CS-2, who was waiting outside of his/her car, walked around to the front passenger side of the unidentified male's vehicle, opened the door, and began to talk to the unidentified male.[3] Approximately one minute later, CS-2 closed the front passenger door and walked back to his/her vehicle holding a cardboard package that he/she had retrieved from the unidentified male's car.

12. Subsequent examination of the cardboard package revealed that it contained a large plastic bag filled with approximately 10,000 blue pills. Based on my training and experience, as well as my review of the communications between CS-1 and PARRA MONTES, I believe that the blue pills contain fentanyl.

13. Based on my meetings with CS-1 and my consensual monitoring of CS-1's communication with the user of the SUBJECT DEVICE, at approximately 1:14 p.m., the user of the SUBJECT DEVICE texted CS-1 to notify him/her that the transaction had been completed, and CS-1 responded by thanking him.

14. Based on my participation in the controlled narcotics purchase on Thursday, March 16, 2023, I know that during the narcotics purchase CS-2 was equipped with an audio/video recording device which captured audio and video of the user of

[3] Law enforcement agents searched CS-2's person and vehicle before the controlled transaction and confirmed that CS-2 did not have any drugs in his/her possession.

the SUBJECT DEVICE inside the green Nissan Rogue. Based on my review of the recording, other communications between CS-1 and the user of the SUBJECT DEVICE, and DMV databases, I believe that JAIMES is the user of the SUBJECT DEVICE.

15. Based on my conversations with other law enforcement agents, I know that JAIMES was arrested by the Buena Park Police Department and Homeland Security Investigations during a controlled narcotics purchase on the morning of Friday, March 31, 2023. An undercover BPPD officer met with JAIMES to purchase approximately 20,000 fentanyl pills. JAIMES used the SUBJECT DEVICE to coordinate this transaction. At the time of his arrest, officers recovered the SUBJECT DEVICE from JAIMES's vehicle. After JAIMES's arrest, he was interviewed at the Buena Park Police Department.

16. I attended BPPD's interview of JAIMES on March 31, 2023. During the interview, JAIMES signed a federal consent-to-search form allowing agents to search the SUBJECT DEVICE.

17. Based on my initial review of the SUBJECT DEVICE pursuant to JAIMES's consent, I know that JAIMES used the SUBJECT DEVICE to facilitate narcotics and firearms transactions with individuals located in the United States and Mexico. For example, JAIMES used the SUBJECT DEVICE to coordinate narcotics transactions on March 16,2023, and March 31, 2023.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

18. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences and vehicles.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residences and vehicles, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their drugs and may keep stashes of drugs in their vehicles in the event of an unexpected opportunity to sell drugs arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and

suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

19. As used herein, the term "digital device" includes the SUBJECT DEVICE.

20. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has

been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

21. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

22. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

//

//

VII. CONCLUSION

23. For all of the reasons described above, there is probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ___ day of May, 2023.

_____

THE HON. ALEXANDER F. MACKINNON
UNITED STATES MAGISTRATE JUDGE